PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087238
(43)Date of publication of application : 20.03.2003

(51)Int.Cl. H04L 9/10
G06F 17/60
G06K 17/00
G06K 19/00
H04L 9/08
H04L 9/32

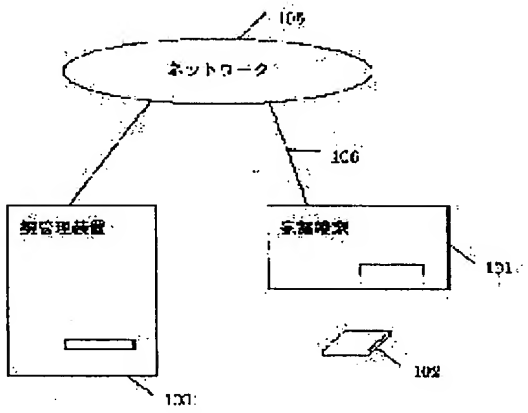
(21)Application number : 2001-274434
(22)Date of filing : 11.09.2001

(71)Applicant : HITACHI LTD
(72)Inventor : EBINA AKIHIRO
KAMIMAKI HIDEKI
SAWAMURA SHINICHI
SUZUKI MASATO
ISHII MASAHITO
MAKIMOTO YOSHINOBU
HIGUCHI TATSUSHI
TAKITA ISAO

(54) SECURITY REALIZING SYSTEM IN DOMESTIC NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system device capable of easily realizing security in a domestic network by preventing communication with a terminal illegally connected to the domestic network.
SOLUTION: A home electric terminal 101 and a key control device 103 are connected to the domestic network 105 via a network connection means 106, the device 103 identifies the terminal 101 by inserting an identification tag 102 into the terminal 101 and a common cipher key for communicating with another home electric terminal 101 connected to the network 105 is acquired to attain safe communication in the network 105.

図1



LEGAL STATUS

[Date of request for examination] 22.09.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－87238
（P2003－87238A）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｇ０６Ｆ　17/60	１７６Ａ　５Ｂ０３５
Ｇ０６Ｆ　17/60	１７６	Ｇ０６Ｋ　17/00	Ｌ　５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｈ０４Ｌ　9/00	６２１Ａ　５Ｊ１０４
19/00			６０１Ｂ
Ｈ０４Ｌ　9/08			６０１Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願2001－274434(P2001－274434)

(22)出願日　平成13年９月11日(2001.9.11)

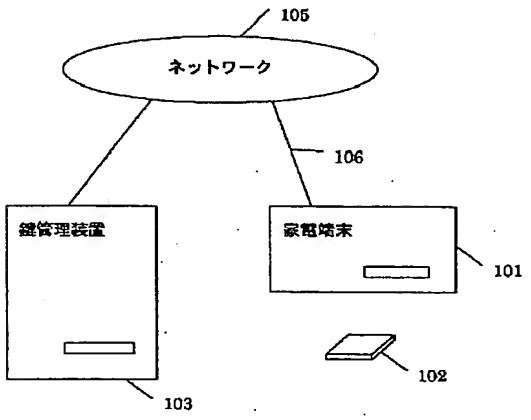
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　海老名　明弘
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　神牧　秀樹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　家庭内ネットワークにおけるセキュリティ実現方式

(57)【要約】
【課題】不正に家庭内のネットワークに接続してきた端末とは通信を行わないようにする事で、家庭内ネットワークにおけるセキュリティを容易に実現するシステム装置を提供する事を目的とする。
【解決手段】家電端末101と鍵管理装置103がネットワーク接続手段106を介して家庭内のネットワーク105に接続されており、認証タグ102を家電端末101に挿入する事で、鍵管理装置103と認証を行い、家庭内のネットワーク105に接続された他の家電端末101と通信を行うための共通暗号鍵を取得する事で、家庭のネットワーク105内で安全な通信が出来るようにする。

図１



【特許請求の範囲】
【請求項１】ネットワーク接続手段を有する家電端末であって、
家庭内でのネットワークを使用するための情報が記録されている認証タグを読み取るためのスロット装置を具備し、認証タグが挿入されることで家庭内に接続された端末装置同士でデータの送受信を行う事が可能となる家電端末。
【請求項２】請求項１に記載の家電端末において、認証タグが家電端末のスロットに挿入されると認証タグに記録されている情報を読み取る手段と、認証タグ内に記録されている情報を家電端末内部に記録しておく手段と、記録した情報の暗号鍵を使用して送信データの暗号化と、受信データの復号化を行う手段を有する家電端末。
【請求項３】請求項１に記載の家電端末において、認証タグ内に記録されているプログラムを家電端末が所有している記録媒体に複製する手段と、複製したプログラムを実行する手段とを有する家電端末。
【請求項４】請求項１に記載の家電端末において、家電端末固有の情報を鍵管理装置に送信する手段と、鍵管理装置で更新された共通暗号鍵を受信し家電端末内に記録されている共通暗号鍵を更新する手段を有する家電端末。
【請求項５】請求項１に記載の鍵管理装置において、家庭内のネットワークに接続されている家電端末の認証を行う手段と、家庭内のネットワークに接続されている家電端末の情報をテーブルとして鍵管理装置内に記録して管理する手段を有する鍵管理装置。
【請求項６】請求項１に記載の鍵管理装置において、家庭内で使用される暗号鍵を生成する手段を有し、前記記載のテーブル情報をもとに家庭内のネットワークに接続された家電端末に配布する手段を有する鍵管理装置。
【請求項７】ネットワークに接続可能な家電端末であって、
認証タグを挿入するスロットと、
前記認証タグに記録された情報を読み出す手段と、
前記読み出された情報を、前記ネットワーク上に送出する手段と、
前記ネットワーク上に送出された情報に対応する情報であって当該家電端末が使用可能であることを示す情報を受信する手段とを有することを特徴とする家電端末。
【請求項８】ネットワークに接続可能な鍵管理装置であって、
認証タグを挿入するスロットと、
前記ネットワークに接続された他の装置を認証する暗号情報を生成する手段と、
前記スロットに挿入された前記認証タグに前記暗号情報を格納する手段とを有することを特徴とする鍵管理装置。
【請求項９】請求項8記載の鍵管理装置であって、
前記ネットワークに接続された他の装置から出力された認証情報を受信する手段と、
前記認証情報を前記鍵管理装置内に格納された認証情報と比較する手段と、
前記比較した結果を前記他の装置に送信する手段とを有することを特徴とする鍵管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、家庭内ネットワークにおけるデータ通信システムに関し、特に、認証タグを使用することでセキュリティ機能を向上させた家庭内ネットワークのデータ通信に関する。
【０００２】
【従来の技術】ネットワークに接続した端末に対してIPアドレスを割り振る方法としてはDHCPのように動的にアドレスを配布する方法が一般的である。しかし、家庭内ネットワークに不正に侵入してきた端末に対してもIPアドレスを割り振ってしまい、ネットワークを自由に使用されてしまう。そこで、不正に家庭内ネットワークに接続した端末に対してネットワークを使用不能にする方法として、DHCPサーバに登録されたMACアドレス以外からの要求には応じないようにする事で、不正な端末に対するアドレスを配布を防ぎ、ネットワークの使用を制限するシステムがある。
【０００３】また、HUBに対してMACアドレスを登録し、登録されたＭＡＣアドレス以外の端末が接続された時、そのポートを通信不能にする事でネットワークへの不正侵入を防止する手段がある。また、特開2001-77811のようにネットワークインターフェースカードにセキュリティ機能を持たせることで、家庭内ネットワークのセキュリティを確保する方法がある。
【０００４】
【発明が解決しようとする課題】しかしながら、DHCPサーバにMACアドレスを登録する方法では、端末に直接IPアドレスを指定する事で容易にネットワークを使用されてしまうという問題があり、IPv6環境では、アドレスは端末毎に自動で生成するため、ネットワーク内のサブネットアドレスを知る必要もなく、容易にネットワークを使用することが可能である。
【０００５】HUBに対してMACアドレスを登録する方法では、ネットワークの管理者が必要であり、接続する機器が増える度にHUBに対して設定を行う必要があるため、家庭内での使用を考えると、ネットワークの知識のない人が管理するのは難しいという問題がある。また、特開2001-77811のようにネットワークインターフェースカードにセキュリティ機能を持たせる方法では、端末毎のネットワークインターフェースカードに対してセキュリティの設定をする必要があるため、ネットワークの管理が難しい事や、ネットワーク内に流れるデータを盗聴、改ざんすることが容易である。

【０００６】本発明はこれらの課題を解決するためのものであり、タグを使用する事で容易に家庭内ネットワークのセキュリティを実現する事を可能にする装置を提供し、家庭内ネットワークに接続された不正な端末にネットワークを使用されないようにすると共に、データを盗聴されることを防ぐことを目的とする。

【０００７】

【課題を解決するための手段】上記目的を解決するために、本発明は、家庭内でのネットワークを使用するための情報が記録されている認証タグを読み取るためのスロット装置を具備し、認証タグがスロットに挿入されると認証タグに記録されている情報を読み取る手段と、認証タグ内に記録されている情報を家電端末内に記録しておく手段と、記録した情報の暗号鍵を使用して送信データの暗号化と、受信データの復号化を行う手段を有し、暗号化データにより鍵管理装置と認証を行い、家庭内の通信に使用される共通暗号鍵を受信する手段を有する事で、ネットワーク接続手段を介して家庭内のネットワークに接続された家電端末同士で暗号化通信を行う事で、送受信を行うデータの機密性を保持する家電端末を実現する。

【０００８】鍵管理装置は、家庭内のネットワークに接続されている家電端末の認証を行う手段と、家庭内のネットワークに接続されている家電端末の情報を管理する手段と、鍵管理装置の情報を認証タグに記録する手段と、通信を行う際の共通暗号鍵の作成を定期的に行い、ネットワークに接続された家電端末に配布する手段を有する事で、家庭内の通信に使用される共通暗号鍵を定期的に変更可能な手段を有する鍵管理装置である。

【０００９】

【発明の実施の形態】以下本発明を図により詳細に説明する。図１は本発明の１例を示すシステムの構成を示している。101はネットワーク接続手段と、認証用タグ内に記録されている家庭内でのネットワーク105を使用するための情報を読み取る手段を備えている家電端末である。例えば、パソコン、インターネット電話、インターネット冷蔵庫、インターネットエアコンなどネットワークに接続することが可能な家電端末がある。102は鍵管理装置103との認証用に用いる暗号鍵と、鍵管理装置103の場所と、認証を行うためのプログラムとが記録されている認証タグである。103は家庭内で使用される共通暗号鍵を管理する鍵管理装置、105は家庭内でのネットワーク、106は有線による1例を示したネットワーク接続手段である。

【００１０】本発明のシステムにおいて、家電端末101は、ネットワークカードなどのネットワークに接続する装置と、家庭内でのネットワーク105を使用するために必要な情報が記録されている認証タグ102を読み取るためのスロット装置を具備し、認証タグ102が挿入されると認証タグ102に記録されている情報を読み取る手段と、認証タグ102内に記録されている情報を家電端末101内に記録しておく手段と、記録した情報の暗号鍵を使用して送信データの暗号化と、受信データの復号化を行う手段を有し、暗号化データを使用して鍵管理装置103と認証を行い、家庭内の通信に使用される共通暗号鍵を受信する手段を有する事で、ネットワーク接続手段106を介してネットワーク105に接続された家電端末同士で暗号化通信を行う事が可能となる家電端末101を実現することが可能である。

【００１１】ここで、暗号鍵とは鍵管理装置103との通信に使用する認証用の鍵であり、共通暗号鍵とは家庭内のネットワーク105に接続された認証タグ101が挿入された家電端末101と通信するために使用する暗号鍵である。また、セキュリティとは、暗号化通信を行うことでデータの機密性を確保するのと、不正に家庭内ネットワーク105侵入してきた他の端末から家庭内の家電端末101を制御されることを防ぐことを意味する。

【００１２】鍵管理装置103は、家庭内のネットワーク105に接続されている家電端末101の認証を行う手段と、家庭内のネットワーク105に接続されている家電端末101の情報を管理する手段と、家庭内でのネットワーク105に参加するための情報を認証タグ102に記録する手段と、通信を行う際の共通暗号鍵の作成を定期的に行い、ネットワーク105に接続された家電端末101に配布する手段を有する事で、家庭内の通信に使用される共通暗号鍵を定期的に変える事でセキュリティ強度を高めることが可能である。

【００１３】認証タグ102に家庭内でのネットワークを使用するために必要な情報が記録されていない場合には、鍵管理装置103のスロットに認証タグ102を挿入する事で、家庭内のネットワーク105を使用するために必要な情報が認証タグ102内に記録される。家庭内のネットワーク105を使用するために必要な情報が記録されている認証タグ102を家電端末101のスロットに挿入する事で、家電端末101は鍵管理装置103と認証の手続きを行い家庭内で通信を行うための共通暗号鍵の受信することで、ネットワーク105に接続された家電端末101と安全に通信を行う事が可能となる。

【００１４】認証タグ102内の家庭内ネットワーク105を使用するために必要な情報を家電端末101内に記録する手法により、認証タグ102を家電端末101に挿入した状態にしておかなくてもよいため、認証タグ102が不正に使用される事を防ぐことが可能で、認証タグ102をネットワーク管理者が管理するだけでネットワーク105のセキュリティを保持することが可能であり、ネットワーク管理者の負担を減らすことが可能となる。

【００１５】家庭内のネットワーク105のデータを暗号化して通信する事により、家庭内のネットワーク105に侵入して接続した不正な端末にデータを傍受たとしても解読することが不可能で、また、不正な端末に家庭内の

家電端末101を不正に制御されたりする心配がない。例えば、無線を用いたネットワーク接続手段106では、従来ではMACアドレスによるアクセス制限や、パスワードによるアクセス制限を行っており、アクセスポイントに接続される機器が増えるたびにMACアドレスの登録をする必要がある。また、ローミング機能を搭載する環境ではすべてのアクセスポイント毎にMACアドレスを登録する必要があり、ネットワーク管理者にとってかなりの手間を要する。また、パスワードによるアクセス制限を行うシステムでは、アクセスポイントの認証用のパスワードを変更するたびにアクセスポイントに接続される機器のパスワードを変更する必要があり、機器使用者にとって複雑な処理を要し、設定を適切に行わなければ容易にネットワーク105に侵入される可能性がある。また、電灯線を用いたネットワーク接続手段106では、家の外にコンセントが設置されている家庭も存在する場合があり、このような場合では、家庭内の人に気づかれずに容易に家庭内のネットワーク105に浸入することが可能である。しかし、本発明では、家庭内ネットワーク105に接続された端末がすべて同じ暗号化データで通信を行うことにより、不正に接続された端末にデータを傍受されたとしても暗号化によりデータの機密性が確保され、容易にネットワーク105のセキュリティを実現できる。

【００１６】認証タグ102のような端末使用者にとって理解しやすいデバイスを使用し、家電端末101に具備されているスロットに認証タグ102を挿入するという簡単な動作を行うことにより、簡単に家庭内のネットワーク105のセキュリティ向上を実現可能となる。認証タグ102は１世帯に１つ配布し、各家庭内のネットワーク105に接続された家電端末101に共通に使用することも可能であり、それぞれの家電端末101に添付する必要もなくなる。

【００１７】セキュリティポリシーに依存するが、家庭内ネットワーク105で使用する暗号鍵の変更をする必要がないネットワーク105においては、鍵管理装置103を設置する必要がなく、認証タグ102に記録されている暗号鍵を使用した暗号化データ通信を行うことも可能となる。インターネットを管理するISP、ASPのサービスとして、鍵管理装置103をサービスプロバイダ側に設置する事により、ISP、ASPに接続する各家庭のネットワーク105を管理することが可能となり、新しいインターネットサービスを提供することも可能となる。

【００１８】モバイル端末のように、家庭外に持ち出し、家庭内の機器と通信を行う場合は、家庭内の端末同士各家庭特有の共通暗号をもちいて通信を行うため、家庭内のネットワーク105と外部のネットワークを接続する部において複雑な認証などのプロセスを踏まなくても簡単に家庭内の家電端末と通信を行う事が可能であり、容易に家電端末を外部ネットワークからモバイル端末により遠隔操作することが可能となる。

【００１９】図2はエアコンの一例を示した家電端末101のハードウェア構成図である。201は認証タグ102がスロット207に挿入されたのを検知するのと、各種のプログラムの実行と、送受信するデータの暗号化・複号化を行うCPU、202はプログラムの実行領域であるメモリ、203はデータの送受信を行うバス、204はネットワークインターフェースの制御と、不揮発性記録媒体の制御と、スロットの制御と、空調機能部208の温度調整や電源のON，OFFなどの制御を行うペリフェラルコントローラ、205はデータの送受信を行うネットワークインターフェース、206はスロット207に認証タグが挿入されたときに起動するプログラムと送受信するデータの暗号化、復号化の処理を行うプログラムの格納と、認証タグ102内に記録されているデータの保存のための不揮発性記録媒体、207は認証タグ102を挿入するためのスロット、208は、制御を行うターゲットである空調機能部である。

【００２０】家電端末101は、スロット207に認証タグ102が挿入されるとCPU201が不揮発性記録媒体206に格納されている認証タグ102内に記録されているデータを家電端末101使用者が容易に書き換え不可能で、ネットワーク105から参照不可能である不揮発性記録媒体206の領域にコピーするプログラムをメモリ202に展開して実行する手段を有する。家電端末101は前記プログラム実行後不揮発性記録媒体206内に記録されている鍵管理装置103と認証を行うためのプログラムと送受信するデータの暗号化、復号化処理を行うプログラムを実行し、認証用の暗号鍵を使用して鍵管理装置103と暗号化通信を行い、MACアドレスやIPアドレスなどの家電端末固有の情報をネットワーク接続手段106を介して鍵管理装置103に送信する手段を有することで、鍵管理装置103で更新された共通暗号鍵をネットワーク接続手段106を介してネットワークインターフェースで受信し不揮発性記録媒体206内に記録されている共通暗号鍵を更新する手段を有する装置である。鍵管理装置103で更新された共通暗号鍵を受信し不揮発性記録媒体206内に記録されている共通暗号鍵を更新する手段を有する事で、共通暗号鍵を定期的に変更する事で高度なセキュリティを実現すことが可能であり、家庭内ネットワーク105に接続されたすべての家電端末101の保持している暗号鍵のデータを変更することが可能である。

【００２１】家電端末101が受信したデータの流れを詳細に述べる。家電端末101はネットワーク105からネットワーク接続手段106を介してネットワークインターフェース205で受信した暗号化データをペリフェラルコントローラ204がバス203を介して、メモリ202に格納する。CPU201は不揮発性記録媒体206に格納されている暗号化、復号化処理を行うプログラムを実行し、暗号化、復号化処理を行うプログラムがメモリ202に格納されている暗号化データを復号化する。CPU201は復号化データを解読し、エアコンを制御する。以上のように動作する事で、

同じ暗号化データで通信を行うことで、家電端末101をネットワーク105を介して制御することが可能となる。

【００２２】家電端末101がデータを送信する流れの詳細を述べる。CPU201は不揮発性記録媒体206に格納されている暗号化、復号化処理を行うプログラムを実行し、メモリ202に格納されている暗号化されていない送信データを暗号化する。CPU201はメモリ202に格納されている暗号化データをペリフェラルコントローラ204を介してネットワークインターフェース205に送信する手段を有し、家庭内のネットワーク205に不揮発性記録媒体206内に記録されている暗号鍵を用いた暗号化データを送信することが可能となる。暗号化、復号化処理を行うプログラムは暗号化アルゴリズムとしてDES(Data Encryption Standard)などで暗号化、復号化を行う。家電端末101は家庭内のネットワーク105に接続していないオフライン時であっても空調機能部208を手動でコントロール可能な手段を有する事で、不揮発性記録媒体206に暗号鍵の情報が記録されていない場合でもエアコンの機能を使用する事は可能である。空調機能部208は家電端末101がエアコンの場合を示した一例であり、テレビやＶＴＲなどの機能を有した部分である。

【００２３】図３は暗号化をハードウェアで行う場合の家電端末101のハードウェア構成図である。209は前記一例で述べたデータの暗号化、復号化の処理を行うプログラムをハードウェア化した暗号化処理部である。暗号化をハードウェアで行う場合の家電端末101がデータを受信する流れの詳細を述べる。家電端末101はネットワーク105からネットワーク接続手段106を介してネットワークインターフェース205で受信した暗号化データをペリフェラルコントローラ204がバス203を介して、メモリ202に格納する。CPU201はメモリ202に格納されている暗号化データをバス203を介して暗号化処理部209に送信する手段を有し、暗号化処理部209は不揮発性記録媒体206内に記録されている暗号鍵を使用して、CPU201から受信した暗号データを復号化する手段と、復号化データをメモリ202に展開する手段を有する。

【００２４】暗号化をハードウェアで行う場合の家電端末101が送信するデータの流れを詳細に述べる。CPU201は、メモリ202に格納されている暗号化されていない送信データを暗号化処理部209に送信する手段と、暗号化処理部209は不揮発性記録媒体206内に記録されている暗号鍵を使用して、CPU201から受信した暗号化されていないデータを暗号化する手段と、ペリフェラルコントローラ204を介してネットワークインターフェース205に送信する手段を有する。以上のようにハードウェアで暗号化、復号化を行うことで、処理を高速に行う事が可能となり、CPU201の処理の負荷を少なくすることが可能となる。

【００２５】図４は鍵管理装置103のハードウェア構成図である。鍵管理装置103は、家電端末101と認証タグ102に記録されている認証用の暗号鍵を使用して認証手続きを行う手段を有し、家電端末101からネットワーク接続手段106を介して送信されるMACアドレスやIPアドレスなどの端末固有の情報を受信し、不揮発性記録媒体206内に登録する手段を有する。また、スロット207に認証タグ102が挿入されると、CPU201が不揮発性記録媒体206に格納されている家庭内のネットワーク105で端末101が鍵管理装置103と通信する際に使用する認証タグ102内の認証用の暗号鍵を書き換えるプログラムをメモリ202に展開して実行する手段を有する事で、新しい認証用の暗号鍵を認証タグ102内に記録することが可能である。また、鍵管理装置103は家庭内のネットワーク105に接続された家電端末101間で通信を行う際に使用する共通暗号鍵を作成する手段と、前記作成された共通暗号鍵を不揮発性記録媒体206に登録されている家庭内のすべての家電端末101に送信する手段を有することで、ネットワーク105に不正に接続された端末に対して共通暗号鍵を知られること無く安全な家庭内のネットワーク105が実現可能であり、容易に家庭内の共通暗号鍵を変更できる。

【００２６】図５は、スロット207周辺の詳細なハードウェア構成図である。301はスロット207に認証タグ102が挿入されたときに割り込み信号をCPU201に送るための割り込み信号線、302は認証タグ102内の記録領域のデータの読み込み信号と、書き込み信号を送るための制御信号線、303は認証タグ102内の記録領域にデータを送信するのと、認証タグ102内の記録領域に記録されているデータを受信するためのデータ信号線、304は認証タグ102に電源を供給するための電源入力線、305はグランド線、306はスロット207に接続されている各種信号線と認証タグ207を接続するための接続端子、307は家庭内のネットワーク105を使用するために必要な情報が記録されている書き換え可能な不揮発性メモリ、308は、認証タグ102を制御するためのマイコンである。

【００２７】上記構成により、家電端末101は家電端末101のスロット207に認証タグ102を挿入すると、認証タグ102の電源入力接続端子306と電源入力線304が接続することで認証タグ102内のマイコン308に電力が供給され、マイコン308は、割り込み信号線301を介して端末装置101のCPU201に割り込み信号を送信し、端末装置101のCPU201が割り込み信号を受信する事で、端末装置101のCPU201は認証タグ102内のメモリ307に記録されている家庭内でのネットワークを使用するための必要な情報を取り出す不揮発性記録媒体206内に格納されているプログラムを実行する手段を有し、前記プログラムが制御信号線302を介して読み込み信号の送信を行い、マイコン308が認証タグ102内のメモリ307に記録されている家庭内でのネットワークを使用するために必要な情報をデータ信号線303を介して家電端末101に送信し、CPU201が不揮発性記録媒体206内に記録する手段を有することで、家電端末101の家庭内でのネットワークを使用するために必要な情

報を受信するための装置家電端末101を実現可能である。

【００２８】同様に上記構成により、鍵管理装置103は、鍵管理装置103のスロット207に認証タグ102が挿入されると、鍵管理装置103のCPU201は不揮発性記録媒体206内に格納されている、鍵管理装置103と認証用に使用する認証用の暗号鍵の作成と、認証タグ102内に記録されている鍵管理装置103と認証を行うために使用する認証用の暗号鍵を書き換えるプログラムを実行する手段を有し、鍵管理装置103のスロット207に挿入されている認証タグ102内のメモリ307に記録されている家庭内でのネットワーク105を使用するために必要な情報をデータ信号線303を介して書き換える手段を有する鍵管理装置103が実現可能である。これにより、認証タグ102を鍵管理装置103のスロット207に挿入する毎に認証タグ102内の認証用の暗号鍵を変更することが可能である。

【００２９】図６は認証タグ102のメモリ307内に記録されているデータを示した図である。601は、認証タグ102内のメモリ307に記録されているデータを示した表である。認証タグ102は、家電端末101のスロット207に認証タグ102が挿入されると、ペリフェラルコントローラ204より読み取り信号をマイコン308が受信し、認証タグ102内のメモリ202に記録されている、鍵管理装置103との認証用の暗号鍵と、鍵管理装置103の場所、例えばIPアドレスなどの家庭内ネットワーク105内での場所と、鍵管理装置103との認証プログラムをマイコン308が読み出し、家電端末101に送信する手段を有する。これにより、家電端末101は認証タグ102内に記録されている家庭内でのネットワーク105を使用するために必要な情報である鍵管理装置103との認証用の暗号鍵と、鍵管理装置103の場所と、認証プログラムを家電端末101内の不揮発性記録媒体206に保存し、鍵管理装置103の場所情報から家庭内ネットワーク105における鍵管理装置103の場所を特定し、認証プログラムを実行する事で、鍵管理装置103と鍵管理装置103との認証用の暗号鍵を使用して、鍵管理装置103と認証を行い、鍵管理装置103から家庭内ネットワーク105での共通暗号鍵を受信する事で、家庭内のネットワーク105に接続された家電端末101と通信を行う事が可能となる。同様に、鍵管理装置103のスロット207に認証タグ102が挿入されると、マイコン308がペリフェラルコントローラ204より書き込み信号を受信し、鍵管理装置103との認証用の暗号鍵と、鍵管理装置103の場所と、認証プログラムを認証タグ102内のメモリ307に書き込む手段を有する。

【００３０】図７は不揮発性記録媒体206に記録されているデータの一例を示した図である。611は、家電端末101の不揮発性記録媒体206内に記録されているデータを示した表である。タグ情報読み取りプログラムは家電端末101のスロット207に認証タグ102が挿入されたときに実行されるすべての家電端末101にプレインストールされているプログラムで、認証タグ102内のメモリ307に記録されている、鍵管理装置103との認証用の暗号鍵と、鍵管理装置103の場所と、認証プログラムを不揮発性記録媒体206内に複製するプログラムである。前記プログラム実行後、不揮発性記録媒体206内に保存した認証プログラムとプレインストールされている暗号化プログラム起動し、認証用の暗号鍵を使用した暗号化データにより鍵管理装置103と通信を行う。認証プログラムは、鍵管理装置103に家電端末101のIPアドレスやMACアドレスなどの家電端末101の情報を登録し、家電端末101はネットワーク接続手段106を介してネットワーク105で使用されている共通鍵暗号を受信し、前記受信した共通暗号鍵を鍵管理装置103との認証用に使用した暗号鍵をネットワーク105で使用されている共通鍵暗号に更新し、次回通信時に暗号化プログラムが共通暗号鍵を使用する事でネットワーク105に接続された他の家電端末101と通信を行う事が可能となる。

【００３１】家電端末101の暗号化処理をハードウェアで行う場合には暗号化プログラムをプレインストールしておかなくてもよい。また、認証タグ102により暗号化プログラムを配布するような仕組にすることも可能である。鍵管理装置101の不揮発性記録媒体206内に暗号鍵を複数個登録可能なテーブルとして持たせる仕組を付加する事で、種類の異なる暗号鍵を保持することが可能であり、特定の家電端末と通信を行うことも可能となる。例えば、製造メーカが家電端末101を販売する際に、製造メーカ独自の端末101ごとに異なる暗号鍵が記録されている認証タグ102を同梱し、家庭内の家電端末101使用者は家庭内で使用する認証タグ102のスロット207への挿入と、同梱されている認証タグ102のスロット207への挿入により、端末101は２つの暗号鍵を持つ事が可能となる。製造メーカは家電端末101に同梱した認証タグ102内に記録されている暗号鍵を使用して通信を行うことで、家庭内の特定の家電端末101のみと通信を行うことが可能であり、特定の家電端末101のメンテナンスや情報収集を安全に、かつ容易に行う事が可能であり、製造メーカが家庭内ネットワーク105に侵入してきても、家庭内ネットワーク105で使用する共通暗号鍵と製造メーカの暗号は異なるため、家庭内ネットワーク105に流れる通信データの傍受や、他の家電端末101の不正制御を防ぐことが可能となる。

【００３２】612は、鍵管理装置103内の不揮発性記録媒体206に記録されているデータを示した表である。鍵管理装置103内の不揮発性記録媒体206には、家庭内のネットワーク105に接続されている家電端末101と通信するために使用する共通鍵暗号と、家庭内ネットワーク105で使用される共通暗号鍵を変更するときに、現在使用している共通暗号鍵を記録しておく過去の家庭内の共通鍵暗号テーブルと、認証タグ102内に記録されている認証用の共通鍵と同じ認証用の共通鍵と、家庭内端末の情報テ

ーブルと、家電端末101と認証を行い家庭内端末の情報テーブルに登録する認証プログラムと、家庭内のネットワーク105内の共通暗号鍵と認証用の暗号鍵を作成する鍵生成プログラムと、鍵管理装置103内と家電端末101内の不揮発性記録媒体206内に記録されている共通暗号鍵を家庭内端末の情報テーブルに含まれる家電端末101にのみ配布する鍵配布プログラムが記録されている。

【００３３】図８は鍵管理装置103内の不揮発性記録媒体206に記録されているテーブル情報の一例を示した図である。621は、過去の家庭内の共通暗号鍵テーブル、622は、家庭内端末の情報テーブルである。

【００３４】鍵管理装置103は家庭内のネットワーク105内の共通暗号鍵を新規に作成を行い、家庭内のネットワーク105に接続された家電端末101に新規に作成された共通暗号鍵を配布する際に、現在の共通暗号鍵を使用して暗号化を行い新規に作成された共通暗号鍵を配布するのと、新規に作成された共通暗号鍵を過去の家庭内の共通暗号鍵テーブル621内の現在の共通暗号鍵に登録する手段を有する。過去の家庭内の共通暗号鍵テーブル621は、家電端末101のＭＡＣアドレスとＩＰアドレスが登録されており、家庭内の共通暗号鍵テーブル621に含まれるＩＰアドレスに対して新規に作成された共通暗号鍵を配布する事で、家庭内のネットワーク105に登録された家電端末101に対してのみ新規に作成された共通暗号鍵を配布することが可能となる。IPv6ネットワークではＭＡＣアドレスよりリンクロカルアドレスを自動で生成する仕組になっているため、ＩＰアドレスのみを家庭内端末の情報テーブル622に登録しておくだけで家電端末101のＭＡＣアドレスを容易に知ることが可能である。

【００３５】図９は、認証タグ102を家電端末101に挿入してから家庭内のネットワーク105内の共通暗号鍵を家電端末101が取得するまでの処理の流れを示した流れ図である。家電端末101のスロット207に認証タグ102を挿入する（ステップ701）。次に、認証タグ102は家電端末101のCPU201に割り込み信号線301を介して割り込み信号を発生する（ステップ702）。CPU201は認証タグ102から送信された割り込み信号を受信すると、不揮発性記録媒体206内に保存されているタグ情報読み取りプログラムを実行する（ステップ703）。タグ情報読み取りプログラムは、認証タグ102内のメモリ307に記録されている情報を不揮発性記録媒体206内にコピーする（ステップ704）。家電端末101は前記ステップ704でコピーした鍵管理装置103のみと通信することが可能な認証用の暗号鍵を使用し、前記ステップ704でコピーした認証プログラムを実行する事で、鍵管理装置103と認証を行う（ステップ705）。鍵管理装置103は家電端末101と認証を行うことで、家電端末101のMACアドレスやIPアドレスを鍵管理装置103内にテーブルとして保存し、家庭内ネットワーク105で使用する共通暗号鍵を家電端末101に送信する（ステップ706）。

【００３６】家電端末101は鍵管理装置103から家庭内ネットワーク105で使用する共通暗号鍵を受信すると、前記ステップ704で不揮発性記録媒体206内にコピーした鍵管理装置103との通信時に使用する認証用の暗号鍵を家庭内のネットワーク105で使用する共通暗号鍵に変更する（ステップ707）。以上のような動作により、家電端末101は、鍵管理装置103に登録されている家庭内のネットワーク105に接続されたその他の家電端末101と通信を行う事が可能となる。例えば、家庭内のネットワーク105がIPv6のネットワーク105においては、家電端末101は家庭内のネットワーク105でのみ使用することが可能なリンクローカルアドレスを自動で生成を行い、家電端末101はこのリンクローカルアドレスを使用して鍵管理装置103と暗号化通信を行い、家庭内のネットワーク105に接続された他の家電端末101と通信を行うための共通暗号鍵に更新することが可能となる。また、外部のネットワークを使用するために必要なグローバルアドレスはルータ機能を持つ端末によりアドレスが配布される仕組であるため、家電端末101は共通暗号鍵を使用して暗号化通信を行うことで、同じ共通暗号鍵を使用した暗号化通信可能なルータよりグローバルアドレスを取得可能となる。このように、家庭内のネットワーク105に不正に接続した家電端末101に対してグローバルアドレスを配布することを防ぐことが可能であり、不正に接続した端末101に家庭内のネットワーク105を不正に使用されることを防ぐことが可能となる。

【００３７】図10は、鍵管理装置103に登録済みの家電端末101が電源をONにした時の動作を示した流れ図である。家庭内ネットワーク105に接続された家電端末101は電源ON時に不揮発性記録媒体206内に記録されている認証プログラムを実行し、不揮発性記録媒体206内に記録されている共通暗号鍵を使用して鍵管理装置103に対して家庭内のネットワーク105で使用されている共通暗号鍵を鍵管理装置103に対して要求する（ステップ801）。鍵管理装置103は不揮発性記録媒体206内の過去の家庭内の共通暗号鍵テーブルの中から、家電端末101と通信可能な過去の共通暗号鍵を使用して家電端末101からの要求を受け取り、鍵管理装置103は前記ステップで要求があった家電端末101のMACアドレスが不揮発性記録媒体206内の家庭内端末の情報テーブル内にあるか判断を行い、家庭内のネットワーク105で使用されている共通暗号鍵を家電端末101に送信する（ステップ802）。

【００３８】家電端末101は鍵管理装置103から家庭内のネットワーク105内で使用されている共通暗号鍵を受信し、不揮発性記録媒体206内に保存する（ステップ803）。家電端末101の電源OFF時などに、家庭内ネットワーク105で使用する共通暗号鍵が更新された場合には、家電端末101は不揮発性記録媒体206内の共通暗号鍵を更新不可能であり、再度電源ON時には他の家電端末101が家庭内のネットワーク105で使用する共通暗号鍵と家電

端末101の共通暗号鍵が異なるため通信を行う事が不可能である。しかし、以上のように家電端末101が動作する事で、家電端末101は電源ON時に家庭内ネットワーク105で使用されている共通暗号鍵に変更することが可能となり、スムーズに通信を行う事が可能となる。

【００３９】

【発明の効果】以上に説明したように、本発明によれば、家庭内で管理された認証タグを家電端末に挿入する事で、複雑な設定や管理をする必要がなく、容易に家庭内のネットワーク105のセキュリティを実現することが可能であり、家庭内のネットワーク105に流れるデータを暗号化することで、家庭内のネットワーク105に侵入した不正な端末からのネットワーク105内に流れるデータを傍受されたとしても解読することが不可能で、ネットワーク105内の家電端末に対する不正な制御を防止出来る。

【図面の簡単な説明】

【図１】　システムの構成図

【図２】　エアコンの一例を示した家電端末101のハードウェア構成図

【図３】　暗号化をハードウェアで行う場合の家電端末101のハードウェア構成図

【図４】　鍵管理装置103のハードウェア構成図

【図５】　スロット207周辺の詳細なハードウェア構成図

【図６】　認証タグ102のメモリ307内に記録されているデータを示した図

【図７】　不揮発性記録媒体206に記録されているデータの一例を示した図

【図８】　テーブル情報の一例を示した図

【図９】　家電端末101に認証タグ102が挿入されたときの動作を示した流れ図

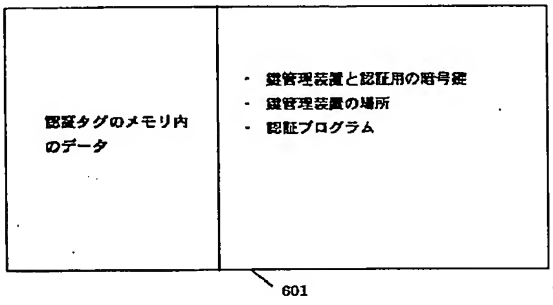
【図１０】　家電端末101の電源ON時の動作を示した流れ図

【符号の説明】

101…家電端末
102…認証タグ
103…鍵管理装置
105…ネットワーク
106…ネットワーク接続手段
201…CPU
202…メモリ
203…バス
204…ペリフェラルコントローラ
205…ネットワークインターフェース
206…不揮発性記録媒体
207…スロット
208…空調機能部
209…暗号化処理部
301…割り込み信号線
302…制御信号線
303…データ信号線
304…電源入力線
305…グランド線
306…接続端子
307…不揮発性メモリ
601…メモリ内のデータ
611…家電端末の不揮発性記録媒体内のデータ表
612…鍵管理装置の不揮発性記録媒体206のデータ表
621…過去の家庭内の共通暗号鍵テーブル
622…家庭内端末の情報テーブル

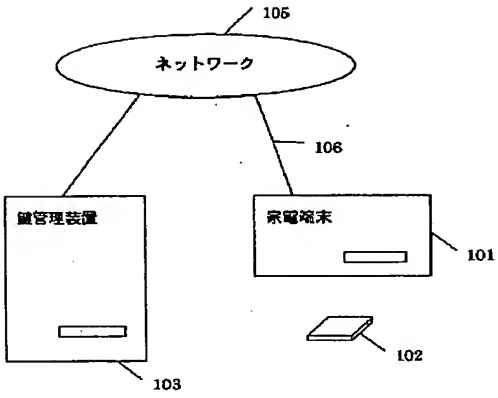
【図６】

図6



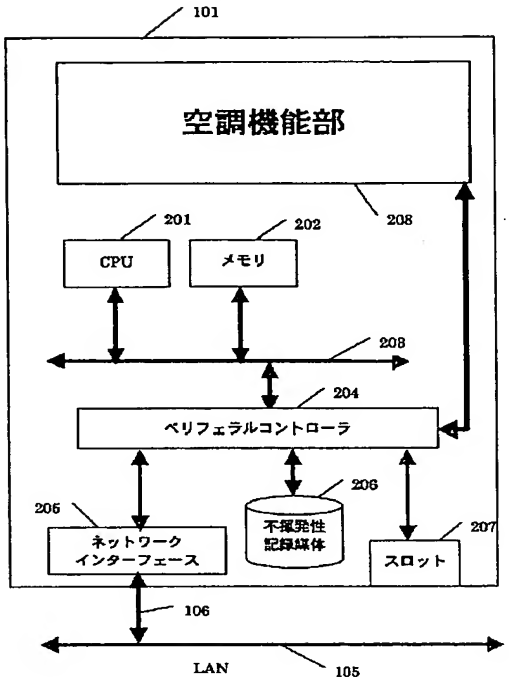
【図1】

図1



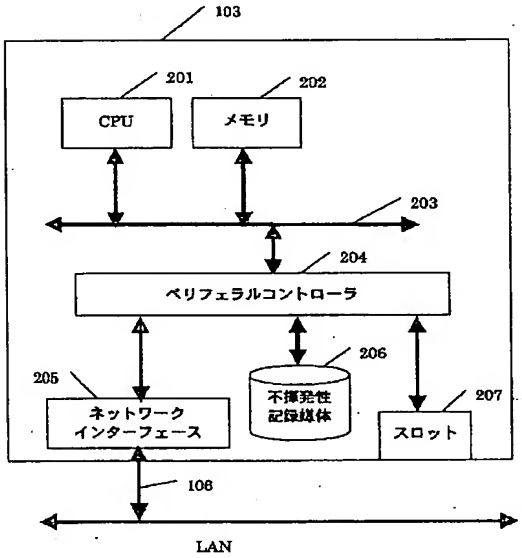
【図2】

図2



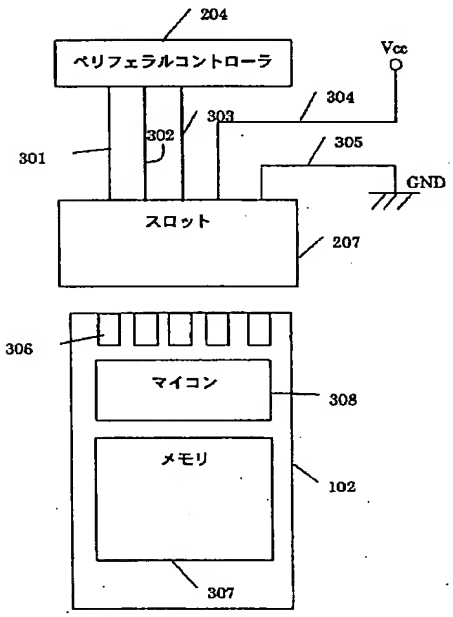
【図4】

図4



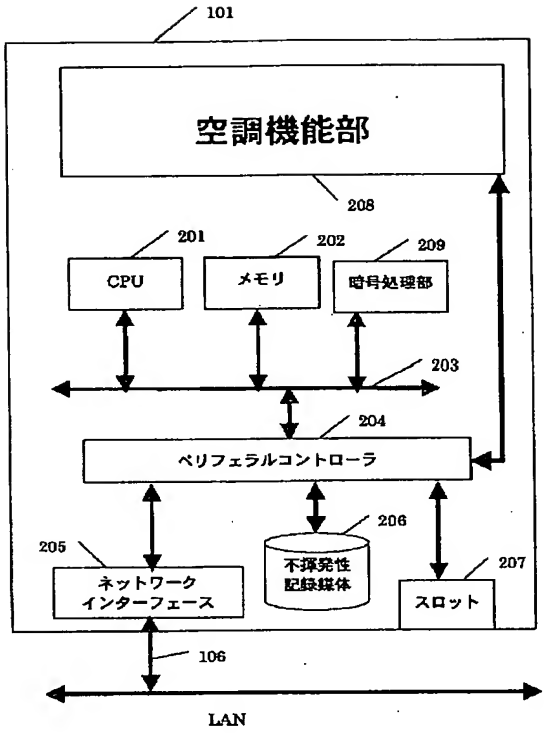
【図5】

図5



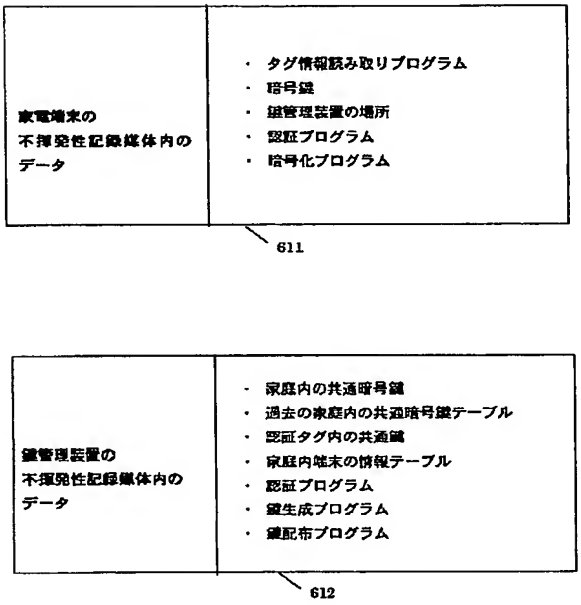
【図3】

図3



【図7】

図7



【図8】

図8

過去の家庭内の共通暗号鍵テーブル

現在の共通暗号鍵	00000000
1つ前の共通暗号鍵	abababab
2つ前の共通暗号鍵	hfushfhs
・・	・・
n つ前の共通暗号鍵	f79gdfra

621

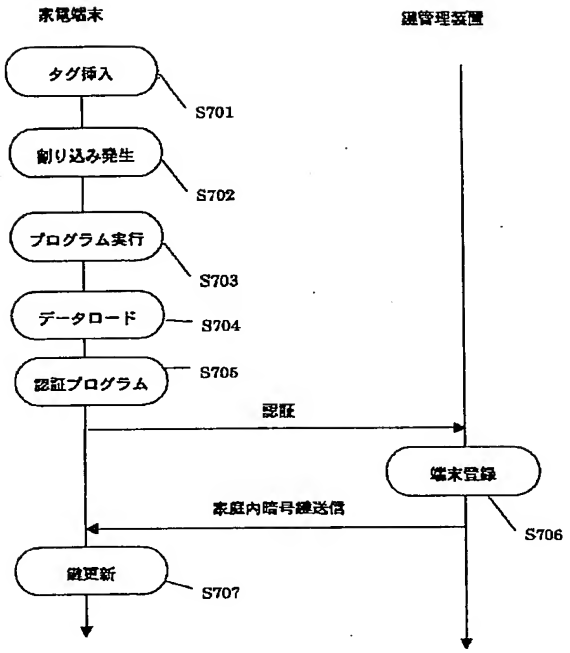
家庭内端末の情報テーブル

MACアドレス	IPアドレス
12-60-97-40-ef-ab	fe80::1260:97ff:fe40:efab
44-45-53-54-00-00	fe80::4445:53ff:fe54:0000
12-34-e2-26-e0-9b	fe80::1234:e2ff:fe26:e09b
12-34-56-89-01-23	fe80::1234:56ff:fe89:0123

622

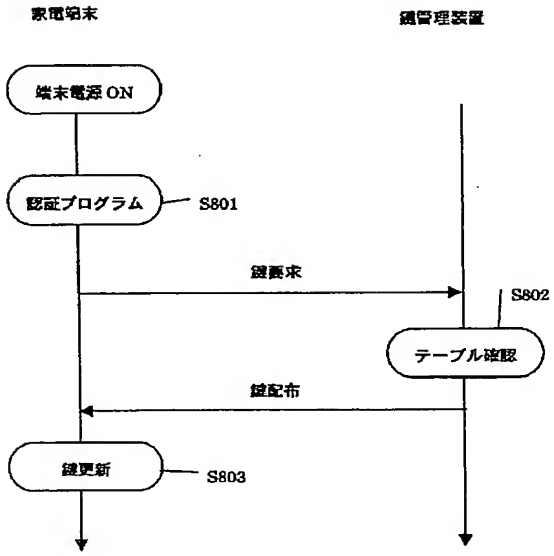
【図９】

図９



【図１０】

図１０



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
H04L 9/32		H04L 9/00	673D	
			675D	
		G06K 19/00	Q	

(72)発明者　澤村　伸一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　鈴木　誠人
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　石井　雅人
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　牧元　喜宣
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　樋口　達志
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　滝田　功
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Fターム（参考）　5B035 BB09 BC00
5B058 CA01 KA31 YA20
5J104 AA04 AA07 AA16 AA34 EA16
KA02 KA21 MA01 MA05 NA02
NA35 NA37 NA40 PA07